



# United States Patent and Trademark Office

UNITED STATES DEPARTMENT OF COMMERCE United States Patent and Trademark Office Address: COMMISSIONER FOR PATENTS P.O. Box 1450 Alexandria, Virginia 22313-1450 www.uspto.gov

APPLICATION NO.	FILING DATE	Е	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,291 .	08/16/2001		Marinus Frans Kaashoek	12221-005001	3137
26161	7590 09/26/2005			EXAMINER	
FISH & RICHARDSON PC P.O. BOX 1022 MINNEAPOLIS, MN 55440-1022			JACKSON, JENISE E		
				ART UNIT	PAPER NUMBER
	•		•	2131	

DATE MAILED: 09/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
!	09/931,291	KAASHOEK ET AL.
Office Action Summary	Examiner	Art Unit
	Jenise E. Jackson	2131
The MAILING DATE of this commu Period for Reply	inication appears on the cover sheet wit	h the correspondence address
A SHORTENED STATUTORY PERIOD WHICHEVER IS LONGER, FROM THE  - Extensions of time may be available under the provisior after SIX (6) MONTHS from the mailing date of this con  - If NO period for reply is specified above, the maximum realiure to reply within the set or extended period for reply any reply received by the Office later than three months earned patent term adjustment. See 37 CFR 1.704(b).	MAILING DATE OF THIS COMMUNIC ns of 37 CFR 1.136(a). In no event, however, may a renuminication.  statutory period will apply and will expire SIX (6) MONT will, by statute, cause the application to become ABAs after the mailing date of this communication, even if the statute of the communication.	CATION.  sply be timely filed  IHS from the mailing date of this communication.  ANDONED (35 U.S.C. § 133).
Status		
1) Responsive to communication(s) fi	led on <u>21 July 2005</u> .	
2a)☐ This action is <b>FINAL</b> .	2b)⊠ This action is non-final.	•
• • •	n for allowance except for formal matte tice under <i>Ex parte Quayl</i> e, 1935 C.D.	
Disposition of Claims		
4)⊠ Claim(s) <u>1,3-9,11-19,21,22 and 24</u> 4a) Of the above claim(s) is/ 5)□ Claim(s) is/are allowed. 6)⊠ Claim(s) <u>1-3,9,11-19,21,22 and 24</u> 7)□ Claim(s) is/are objected to. 8)□ Claim(s) are subject to restr	are withdrawn from consideration.  -27 is/are rejected.	
Application Papers		
9)☐ The specification is objected to by t	he Examiner.	
10) The drawing(s) filed on is/are		
., , , , , , , , , , , , , , , , , , ,	ection to the drawing(s) be held in abeyand	, ,
Replacement drawing sheet(s) includir  11) The oath or declaration is objected	ng the correction is required if the drawing(s to by the Examiner. Note the attached	
Priority under 35 U.S.C. § 119		
<ul><li>2. Certified copies of the priorit</li><li>3. Copies of the certified copies application from the Internat</li></ul>	n for foreign priority under 35 U.S.C. §  y documents have been received.  y documents have been received in Ap  s of the priority documents have been i  ional Bureau (PCT Rule 17.2(a)).  ion for a list of the certified copies not re	pplication No received in this National Stage
Attachment(s)		
1) Notice of References Cited (PTO-892)		ummary (PTO-413)
2) Notice of Draftsperson's Patent Drawing Review 3) Information Disclosure Statement(s) (PTO-1449 of Paper No(s)/Mail Date 69212003	· · · · · · · · · · · · · · · · · · ·	)/Mail Date formal Patent Application (PTO-152) 

Application/Control Number: 09/931,291

Art Unit: 2131

#### **DETAILED ACTION**

### Claim Rejections - 35 USC § 103

- 1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
  - (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.
- 2. Claims 1, 3, 5-6, 9, 12-13, 18-19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Malan et al(6,944,673).
- 3. As per claims 1, 9, 18, 21, Messmer teaches a central control center(i.e. Counterpane data center)(see lines 26-28) to coordinate thwarting attacks(see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network(see lines 12-15), the customers network is the victim data center. Messmer teaches a communication device(i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors(see lines 23-26), dispersed through the network(see lines 23-27), the monitors sending data collected from the network over a hardened redundant network(see lines 23-28). Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center(see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network(12-26), the central control center has its own network, that is in California or

Application/Control Number: 09/931,291

Art Unit: 2131

Virginia, where the data from the monitors is collected and sent to the data center(see lines 26-28). Messmer teaches a computer system that includes a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic(see lines 28-32). Messmer is silent on, an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. However, Malan et al. discloses analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center(see col. 4, lines 60-65, col. 5, lines 43-53, col. 10, lines 56-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Malan's analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center with Messmer, the motivation is that protecting a network from undesirable network traffic is useful which combats denial of service attacks, by having a Dos scrubber can identity malicious traffic, and prevent it from infecting the network(see col. 4, lines 36-65, col. 5, lines 30-53 of Malan et al.)

- 4. As per claim 3, Messmer teaches wherein the data analyzed by the control center is collected statistical information about network flows(see lines 29-30).
- 5. As per claim 5, Messmer teaches wherein the control center is a hardened site, because the data collected is sent in encrypted form to the central control center(see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network(12-26), the central control center has its own network, that is in California or

Art Unit: 2131

Virginia, where the data from the monitors is collected and sent to the data center(see lines 26-28).

- 6. As per claim 6, Messmer teaches wherein the monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network(see lines 12-25), the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network(see lines 26-30).
- 7. As per claims 12, 19, Messmer teaches receiving and analyzing are performed by a control center coupled to the data collectors via the hardened, redundant network(see lines 12-28).
- 8. As per claim 13, Messmer teaches wherein plurality of monitoring devices(see lines 13-26); are data collectors dispersed throughout the network and at least one gateway device that is disposed adjacent the victim site to protect the victim (see lines 6-26), and wherein analyzing includes analyzing at a control center data from the at least one gateway and the data collectors dispersed throughout the network(see lines 26-30).
- 9. Same Motivation applies above(see claim 1). Claim 18, is rejected under the same basis as claim 1. Further, Claim 18, is rejected for Malan disclosing determining a filtering process to eliminate the malicious traffic from entering the victim center; and aggregate traffic information and coordinating measures to locate and block sources of an attack(see col. 4, lines 60-65, col. 5, lines 43-53, col. 7, lines 1-6).
- 10. As per claim 21, limitations have already been addressed(see claim 1 and 18).

Application/Control Number: 09/931,291 Page 5

Art Unit: 2131

## Claim Rejections - 35 USC § 103

- 11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
  - (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.
- 12. Claims 7-8, 14-16, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Hill et al.
- 13. As per claims 7, 14, 24 Messmer does not disclose classifying attack. However, Hill et al. does disclose classifying attacks(see col. 5, lines 66-67, col. 6, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Hill et al. classifying attacks within Messmer, because classifying attacks displays attack information in a usable and quickly interpretable form to a network manager while minimizing the loading on the computer(see col. 2, lines 45-50 of Hill et al.). Therefore, by classifying attacks provides a network manager with knowledge of the severity and overall nature of the attack(see col. 2, lines 53-60 of Hill et al.).
- 14. As per claims 8, 15, 25 same motivation as above. Hill et al. discloses wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing(see fig. 3, sheet 3, fig. 7, sheet 6).
- 15. As per claim 16, Messmer teaches sending requests to gateways to send data pertaining to an attack to the control center(see lines 14-27).

Application/Control Number: 09/931,291 Page 6

Art Unit: 2131

## **Response to Amendment**

16. As far as the subject matter that was objected to new art has been applied to reject the limitations.

17. Second, the Applicant has brought in Mell state that the claims do not teach the limitations of art that was used. However, the Examiner does not see how the reference Mell applies to, Messmer and Hill. Furthermore, the Applicant has not argued specifically how the prior art of record does not apply to the claims. Therefore, Remarks based on Mell are moot.

#### Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/931,291

Art Unit: 2131

September 21, 2005

Page 7

Primary Examiner

a 123 tos